REMARKS

Reconsideration of the application is requested.

Claims 1-27 remain in the application. Claims 1-27 are subject to examination. Claims 1 and 18 have been amended.

Under the heading "Claim Rejections – 35 USC § 103" on page 4 of the above-identified Office Action, claims 1-27 have been rejected as being unpatentable over U.S. Patent No. 6,424,954 to Leon and further in view of U.S. Patent No. 6,557,104 to Vu et al. under 35 U.S.C. § 103.

Support for the changes to claims 1 and 18 can be found by referring to claims 1 and 18, as previously presented, and to the specification at page 24, lines 11-15 and at page 5, lines 8-25.

Claim 1 now includes a removable authorization device for providing an authorization of an initialization of said mailing machine, and claim 1 specifies that the initialization includes inputting initialization data to said mailing machine.

The Examiner has referred to column 37, lines 46-67 of Leon, which teaches an input element 238 connected to an input circuit for initiating an action. This input element 238 can be a switch, push button, or key. When the input

element 238 is actuated, the secure metering device (SMD) generates an indicium and directs a printer 152 to print the indicium.

The cited teaching of Leon is totally unrelated to a removable authorization device for providing an authorization of an initialization of said mailing machine, wherein the initialization includes inputting initialization data to said mailing machine.

The Examiner has also cited the teaching of Vu.

Vu teaches that the prior art method of using a physical smart card to provide a secure environment for storing and processing a secret key has cost disadvantages and that the prior art method of using a virtual smart card to provide a secure environment for storing and processing a secret key has various security disadvantages.

Vu teaches storing a cryptographic key and perhaps storing associated algorithms on a token. Vu teaches that when an application program running on a first computer needs to access a secure computer system or network:
1) booting up the computer in a secure management mode (SSM); and
2) loading the cryptographic key and associated algorithms onto the computer while the computer is booting up.

Since no programs can access the cryptographic key and associated algorithms during boot up, the information is secure (See column 5, lines 24-30 and column 4, lines 21 through column 5, line 23 of Vu).

Vu does not relate to a mailing machine, but rather relates to a computer with an operating system running many different application programs. Some of these programs may have been downloaded by the user and may be unwanted spyware. The mailing machine of Leon is not a computer. There is no risk of unwanted programs being downloaded onto the machine.

Further, the mailing machine of Leon is completely configured at the factory. In fact Leon specifically teaches that the FIT flag, which was previously installed, is removed at the factory and a tamper evident enclosure is sealed (column 13, lines 59-62). With the FIT flag removed, the configuration could not be changed. The teaching of Vu is not relevant to the mailing machine of Leon.

Further, Vu does not relate to providing an authorization of an initialization of said mailing machine. Nor does the teaching relate to an authorization of an initialization of a computer. Vu very clearly relates to a method for processing cryptographic keys in a secure environment by storing the key externally to a computer and by processing the key only when the computer is booting up in a secure management mode. Processing the cryptographic keys is performed to allow an application program running on a first computer to access a secure computer or a network communicating with the first computer.

Similar to Leon, the cited teaching of Vu is totally unrelated to the limitations of claim 1 that were copied above. Vu does not teach a removable authorization device for providing an authorization of an initialization of said mailing machine, wherein the initialization includes inputting initialization data to said mailing machine.

Applicant points out that Leon does teach using cryptographic keys for secure data transfer (See column 4, lines 43-55). Leon goes on to teach that the cryptographic module is enclosed in a tamper evident enclosure and that removal of the cryptographic module is only possible by destroying the enclosure. It seems pretty clear that Leon would not want to have a removable cryptographic module since they want to prevent physical access to the cryptographic keys and to the cryptographic module which performs the secure processing. Therefore it appears that one would not want to use the token taught by Vu to store the cryptographic keys.

More importantly, even if the token of Vu were used to store a cryptographic key, it would be used for secure data transfer. There is no teaching or suggestion to use the token of Vu to provide authorization of an initialization of the mailing machine.

Still further applicant notes that the initialization of the metering device of Leon is performed at the factory under controlled and secure conditions. No

unknown or spyware programs are installed in the metering device of Leon. Applicant once again points out that there is no need or desire to store a cryptographic key externally from Leon's metering device.

One of ordinary skill in the art considering the teachings in Leon and Vu simply could not have obtained a suggestion leading to the invention as defined by claim 1.

Claim 18 includes a step of providing an authorization of an initialization of the mailing machine with a removable authorization device, wherein the initialization includes inputting initialization data to the mailing machine. These limitations are similar to those of claim 1 that have been discussed above, and claim 18 is believed to be patentable for the reasons discussed above with regard to claim 1 and the teachings in Leon and Vu.

It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claims 1 or 18. Claims 1 and 18 are, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 1 or 18.

In view of the foregoing, reconsideration and allowance of claims 1-27 are solicited.

In the event the Examiner should still find any of the claims to be unpatentable, counsel would appreciate receiving a telephone call so that, if possible, patentable language can be worked out.

Please charge any fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner Greenberg Stemer LLP, No. 12-1099.

Respectfully submitted,

/Mark P. Weichselbaum/
Mark P. Weichselbaum
(Reg. No. 43,248)

MPW:cgm

October 20, 2010

Lerner Greenberg Stemer LLP
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: (954) 925-1100
Fax: (954) 925-1101